

Attorney Docket # 2132-25PCON

Express Mail #EL470951471US
Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Janne LINKOLA et al.
Serial No.: n/a
Filed: concurrently
For: Method and Apparatus for Remotely
Accessing a Password-Protected Service in
a Data Communication System



LETTER TRANSMITTING PRIORITY DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

SIR:


In order to complete the claim to priority in the above-identified application under 35 U.S.C. §119, enclosed herewith is the certified documentation as follows:

Application No. **973528**, filed on August 27, 1997, in Finland, and Application No. **PCT/FI98/00653** filed on August 25, 1998 as an International PCT patent application, upon which the priority claim is based.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By


Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: February 25, 2000

Helsinki 16.2.2000

By Express Mail
No. EL470951471US

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT



Hakija
Applicant

Telecom Finland Oy
Helsinki

Patenttihakemus nro
Patent application no

973528

Tekemispäivä
Filing date

27.08.1997

Kansainvälinen luokka
International class

H04L 9/32

Keksinnön himitys
Title of invention

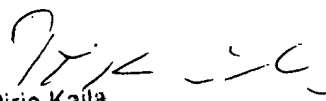
"Menetelmä palvelun käyttämiseksi tietoliikennejärjestelmässä ja
tietoliikennejärjestelmä"

Hakijan nimi on hakemusdiaariin 05.01.1999 tehdyn nimenmuutoksen
jälkeen **Sonera Oy**.

The application has according to an entry made in the register
of patent applications on 05.01.1999 with the name changed into
Sonera Oy.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä
patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä,
patenttivaatimuksista ja tiivistelmästä.

This is to certify that the annexed documents are true copies of the
description, claims and abstract originally filed with the Finnish Patent
Office.


Pirjo Kaila
Tutkimussihteeri

CERTIFIED COPY OF
PRIORITY DOCUMENT

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5204
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5204
FIN-00101 Helsinki, FINLAND

JCS25 U.S. PTO
09/513704
02/25/00

MENETELMÄ PALVELUN KÄYTTÄMISEKSI TIETOLIIKENNEJÄRJESTELMÄSSÄ JA TIETOLIIKENNEJÄRJESTELMÄ

Keksinnön kohteena on patenttivaatimuksen 1
5 johdanto-osassa määritelty menetelmä. Edelleen keksinnön kohteena on patenttivaatimuksen 6 johdanto-osassa määritelty järjestelmä.

Monet yleisessä televerkossa tai muissa data-verkoissa tarjottavat palvelut edellyttävät käyttäjän
10 luotettavaa tunnistamista. Tällaisia ovat esimerkiksi pankkipalvelut. Palveluun saattaa liittyä merkittäviä taloudellisia vaikutuksia ja palvelun tarjoaja haluaa tällöin varmistua käyttäjän identiteetistä ennen kuin hän tarjoaa palvelun.

15 Hyvin usein, esimerkiksi juuri pankkipalvelujen yhteydessä, käyttäjä tunnistetaan salasanojen avulla. Tavallisesti nämä salasanat ovat kertakäyttöisiä. Palvelun tarjoaja, tai hänen valtuuttamansa tunnistava taho, on antanut käyttäjälle etukäteen joukon
20 salasanaja (esimerkiksi nelinumeroisia lukuja), joista asiakas palveluja tarvitessaan käyttää aina yhden. Kun salasanat alkavat loppua, palvelun tarjoaja (tai hänen valtuuttamansa taho) lähettää käyttäjälle listan uusia salasanaja. Täten käyttäjällä on hallussa aina riittä-
25 västi salasanaja lähitulevaisuuden tarpeita silmällä pitäen.

Aiemmin tunnetuille ratkaisuille on tyypillistä se, että asiakas joutuu syöttämään kertakäyttöisen salasanan käsin palvelinlaitteelle kytkeytyessään.
30 Usein tämä tapahtuu esimerkiksi puhelin kojeen näppäimiä painelemalla, jotka aiheuttavat tiedon välittymisen palvelimelle äänitaajuuslähetystä, ns. DTMF-koodeja (dual tone multifrequency), käyttämällä. On myös monia muita tunnettuja salasanan välitysmetodeja,
35 kuten esimerkiksi GSM-verkon lyhytviestipalvelu. (GSM, Global System for Mobile Communications, GSM-verkolla tarkoitetaan tässä esityksessä mitä tahansa GSM-

spesifikaatioihin perustuvaa matkaviestinverkkoa.) Olennaista kuitenkin on nimenomaan se, että käyttäjän täytyy ne itse käsin syöttää. Tämä on käyttäjän kannalta usein varsin hankalaa.

5 Toinen aikaisemmin tunnetuille ratkaisuille tyypillinen piirre on, että palvelun tarjoaja joutuu lähettämään uudet salasanaat melko epäturvallista tiedonsiirtomekanismia käyttäen. Yleisimmin käytössä oleva metodi on posti. Ongelmana on, että salasanaat sisältävä kirje voi joutua vääriin käsiin.

10 Keksinnön tarkoituksena on poistaa edellä mainitut ongelmat.

 Erityisesti keksinnön tarkoituksena on tuoda esiin täysin uudentyyppinen menetelmä ja järjestelmä
15 salasanojen siirtämiseksi käyttäjän puhelinlaitteen ja palvelinlaitteen välillä.

 Edelleen keksinnön tarkoituksena on helpottaa salasanoja tarvitsevien palvelujen käyttöä vähentämällä käyttäjän interaktiota vaativien rutiinien lukumäärää kyseisten palveluiden käytön yhteydessä tekemättä
20 kompromisseja palveluiden turvallisuuden suhteen.

 Keksinnön mukaiselle menetelmälle on tunnusomaista se, mitä on esitetty patenttivaatimuksessa 1. Keksinnön mukaiselle järjestelmälle on tunnusomaista
25 se, mitä on esitetty patenttivaatimuksessa 6.

 Keksinnön mukaisessa menetelmässä palvelun käyttämiseksi tietoliikennejärjestelmässä, jossa palvelun tarjoaja antaa palvelun käyttäjälle joukon kertakäyttöisiä salasanoja, joita käyttäen käyttäjä pääsee käyttämään palvelua tele- ja/tai dataverkon välityksellä, päätelaitteella luodaan yhteys palvelinlaitteeseen ja lähetetään salasana palveluun kytkeydyttäessä, tunnistetaan salasana ja sallitaan ja/tai estetään palvelun käyttö annetun salasanan perusteella.

35 Keksinnön mukaisesti menetelmässä tallennetaan päätelaitteeseen salasanajoukko, valitaan oikea salasana tallennetusta salasanajoukosta ennalta määrättyyn

palveluun kytkeydyttäessä, ja liitetään salasana automaattisesti päätelaitteesta palvelinlaitteeseen siirrettävään yhteydenottosignaaliin.

Vastaavasti keksinnön mukaisesti järjestelmässä päätelaitteeseen kuuluu välineet salasanajoukon tallentamiseksi ja oikean salasanan valitsemiseksi tallennetusta salasanajoukosta ennalta määrättyyn palveluun kytkeydyttäessä salasanan automaattiseksi liittämiseksi päätelaitteesta palvelinlaitteeseen siirrettävään yhteydenottosignaaliin.

Keksinnön etuna on, että se tuo esiin täysin uudentyyppisen salasanojen siirtomekanismin käyttäjän puhelinlaitteen ja palvelinlaitteen välillä. Edelleen keksinnön etuna on, että se helpottaa salasanoja tarvitsevien palvelujen käyttöä vähentämällä käyttäjän interaktiota vaativien rutiinien lukumäärää kyseisten palveluiden käytön yhteydessä. Tämä tehdään ilman kompromisseja palveluiden turvallisuudessa.

Menetelmän eräässä sovelluksessa kirjataan salasanajoukosta käytetyt salasanat.

Menetelmän eräässä sovelluksessa päivitetään päätelaitteessa olevaa salasanajoukkoa palvelinlaitteelta tele- ja/tai dataverkon välityksellä.

Menetelmän eräässä sovelluksessa tilataan uusi salasanajoukko automaattisesti palvelinlaitteelta edellisen salasanajoukon tultua käytetyksi.

Menetelmän eräässä sovelluksessa tallennetaan päätelaitteeseen useita eri palveluja vastaavia salasanajoukkoja, ja valitaan yhteydenmuodostuksessa kulloistakin käytettävää palvelua vastaava salasanajoukko.

Järjestelmän eräässä sovelluksessa päätelaitteeseen kuuluu välineet salasanajoukon käytettyjen salasanojen kirjaamiseksi.

Järjestelmän eräässä sovelluksessa palvelinlaitteeseen kuuluu välineet salasanajoukon päivittämiseksi päätelaitteelle tele- ja/tai dataverkon välityk-

sellä, ja että päätelaitteeseen kuuluu välineet salasanajoukon vastaanottamiseksi.

Järjestelmän eräässä sovelluksessa päätelaitteeseen kuuluu välineet uuden salasanajoukon automaattiseksi tilaamiseksi palvelinlaitteelta edellisen salasanajoukon tultua käytetyksi.

Järjestelmän eräässä sovelluksessa päätelaitteeseen kuuluu välineet useita eri palveluja vastaavien salasanajoukkojen tallentamiseksi.

Järjestelmän eräässä sovelluksessa päätelaitteeseen kuuluu välineet kulloistakin käytettävää palvelua vastaavan salasanajoukon valitsemiseksi.

Järjestelmän eräässä sovelluksessa tietoliikennejärjestelmään kuuluu kiinteä verkko ja päätelaite on kiinteän verkon telepätelaite, kuten puhelin.

Järjestelmän eräässä sovelluksessa tietoliikennejärjestelmään kuuluu matkaviestinverkko, kuten GSM-verkko, ja päätelaite on matkaviestin, kuten GSM-puhelin.

Järjestelmän eräässä sovelluksessa päätelaite on GSM-puhelin, ja että välineet mainittujen salasanojen hallintatoimintojen käyttämiseksi on järjestetty tilaaja-identiteettimoduliin, kuten SIM-korttiin.

Järjestelmän eräässä sovelluksessa tilaaja-identiteettimodulin ja palvelinlaitteen välisessä yhteydenmuodostuksessa salasanojen välitys on järjestetty soitettun tilaajanumeron avulla.

Järjestelmän eräässä sovelluksessa tilaaja-identiteettimodulin ohjelmavälineet on järjestetty tunnistamaan palvelun sen tunnistetiedon, kuten puhelinnumeron, perusteella, ja lisäämään yhteydenmuodostuksessa palvelun puhelinnumeron loppuun joukon lisänumeroita, jotka muodostavat salasanan.

Järjestelmän eräässä sovelluksessa tilaaja-identiteettimoduliin on järjestetty palveluhakemisto, joka sisältää tiedot palveluista, palvelujen tunniste-

tiedoista ja palvelujen yhteydessä käytettävien salasana-
natiedostojen nimistä.

Järjestelmän eräässä sovelluksessa palveluhakemistoon on järjestetty kutakin palvelua varten osoitin, joka on järjestetty osoittamaan salasanajoukon
5 ensimmäistä käyttämätöntä salasanaa ja ko. salasanan tultua käytetyksi siirtymään osoittamaan järjestyksessä seuraavaa käyttämätöntä salasanaa.

Järjestelmän eräässä sovelluksessa välineisiin uusien salasanojen tilaamiseksi ja niiden siirtämiseksi palvelinlaitteen ja tilaajaidentiteettimodulin välillä kuuluu GSM-verkon lyhytsanomapalvelu (SMS-PP-palvelu).

Seuraavassa keksintöä selostetaan yksityiskohtaisesti sovellutusesimerkin avulla.

Keksintö perustuu siihen, että puhelinkojeessa on toiminnallisuuden mahdollistava lisämoduuli (fyysinen tai looginen), joka luo palveluun liittyvän yhteydenoton yhteydessä puhelinkojeen ja palvelinlaitten väliseen liikennöintiin lisäsignaaleja ja/tai puhelinkojeen ja palvelinlaitteen välisen liikennöintiin lisäkenttiä ja/tai komponentteja tai vastaavia, joissa kertakäyttöinen salasana siirretään. Tämä tapahtuu automaattisesti käyttäjän asiaa huomaamatta. Moduuli pitää kirjaa kulloinkin käytetyistä salasanoista ja tuntee täten, mikä on oikea salasana kullakin kytkeytymiskerralla. Käyttäjä kokee tällaiset palvelut helpompina käyttää, kuitenkin ne ovat tietoturvaltaan samaa tasoa niiden palveluiden kanssa, joissa käyttäjän täytyy itse syöttää salasanat. Lisämoduuli osaa myös vastaanottaa uudet salasanat palvelinlaitteelta sekä se
25
30 osaa tarvittaessa jopa tilata uudet salasanat.

Puhelinkojeessa oleva lisämoduuli voi tukea useita yhtäaikaaisia kertakäyttöisiä salasanoja tarvitsevia palveluita. Tätä varten lisämoduulissa on ns. tuettujen palvelujen hakemisto (lyhyemmin: palveluhakemisto), jonka avulla kertakäyttöisiä salasanoja tar-

vitseva palvelu tunnistetaan ja jonka avulla löydetään myös oikea salasanojen lista ja jonka avulla myös oikea paikka kyseisestä listasta löydetään.

Keksinnön paras toteutusmuoto on matkaviestin, kuten GSM-puhelin, jonka tilaajaidentiteettimoduulissa eli SIM-kortilla sijaitseva SIM Application Toolkit -komentoja käyttävä sovellus saa kuvatun lisätoiminnallisuuden aikaan. SIM-kortin ja palvelinlaitteen välisen palveluyhteyden muodostuksen yhteydessä käytettävä salasanojen välitysmekanismi on soitettun tilaajanumeron eli ns. B-tunnisteen käyttö. SIM-kortilla oleva sovellus käyttää TS GSM 11.14 -spesifikaatiossa määriteltä Call Control by SIM -komentoa ja käytännössä sovellus käsittelee jokaisen soitettun tilaajanumeron eli vertaa sitä palveluhakemistoon tallennettuihin numeroihin ja havaitessaan puhelun suuntautuvan johonkin tallennetuista numeroista lisää puhelinnumeron loppuun tarvittavan määrän lisänumeroita, joihin kertakäyttöinen salasana on koodattu. Kun esimerkiksi soittaja yrittää soittaa numeroon 0800-XYZ-123456, SIM-kortilla sijaitseva sovellus muuttaakin numeron muotoon 0800-XYZ-123456-KLMN. Muutettun numeron neljä viimeistä numeroa (KLMN) ovat SIM-kortin lisäämä kertakäyttöinen salasana.

Palveluhakemisto voi olla toteutettu erikoistiedostona SIM-kortilla. Erikoistiedosto sisältää tiedon tuetuista palveluista, näiden tunnistetiedoista ja palveluiden yhteydessä käytettävien salasanatiedostojen nimistä. Lisäksi palveluhakemisto sisältää kunkin palvelun osalta osoittimen siihen kohtaan, jossa salasanojen käytössä ollaan. Taulukossa 1 on esitetty esimerkki kyseisessä tiedostossa sijaitsevista informaatioelementeistä.

Esimerkiksi palvelu 1 tunnistetaan siitä, että käyttäjä soittaa numeroon 0800123. Sovellus tietää tällöin, että numeron loppuun tulee lisätä kertakäyttöinen salasana, joka löytyy tiedostosta 2FF5. Tällä

kertaa käytettävä salasana on kyseisen tiedoston kolmastoista salasana.

Palvelutunniste	Metodi	Metodiin liittyvät tunnisteet	Salasana-tiedoston nimi	Osoitin	Salasanojen kokonaismäärä
1	BID	0800123	2FF5	13	100
2	BID	0800456	2FF4	11	100
3	SMS	SMSC:+02 0202800 BID:8756	2FF6	2	9

5

Taulukko 1 Keksinnön eräässä toteutusmuodossa käytetty palveluhakemisto

Yleisessä televerkossa sijaitseva palvelinlaite saa tiedon kertakäyttöisestä salasanasta puhelinverkon signaloinnissa. Palvelinlaite ottaa B-tunnisteen neljä viimeistä numeroa ja olettaa ne käyttäjän kertakäyttöiseksi salasanaksi. Palvelinlaite vertaa saamaansa kertakäyttöistä salasanaa omaan tietoonsa käyttäjän seuraavasta salasanasta. Tämä tapahtuu jo nykyisin tunnetuin menetelmin.

Jos palvelu vaatii käyttäjätunnuksen käyttämisestä palveluun kytkeydyttäessä, palveluhakemistossa voi olla tallennettuna myös käyttäjätunnukset kullekin palvelulle. Käyttäjätunnus voidaan lisätä yhteydenotto-signaaliin samaan tapaan kuin salasana.

Uusien salasanojen siirtoon palvelinlaitteen ja SIM-kortilla sijaitsevan keksinnön mukaisen sovelluksen välillä voidaan käyttää GSM-verkon SMS-PP palvelua. Mahdollinen SIM-kortilta tuleva uusien salasanojen tilaus tapahtuu SMS-PP/MO (Mobile Originated) -palvelulla ja salasanojen siirto SIM-kortille tapahtuu SMS/PP-MT -palvelua hyväksi käyttäen.

Sovelluksen toiminnallisuus jakautuu kolmen lohkon kesken. Ensimmäinen lohko, lisääjälohko, tun-

nistaa kertakäyttöisen salasanan lisäystarpeen ja välittää salasanan etsimispyynnön salasananetsintälohkolle. Kun etsintälohko on löytänyt oikean salasanan lisääjälohko lisää saamansa kertakäyttöisen salasanan
5 B-tunnisteseen ja päästää puhelun etenemään puhelin-kojeesta ulos.

Salasanojen etsintälohko saa lisääjälohkolta tiedon salasanan etsintätarpeesta. Salasanan etsintälohko käyttää hyväkseen palveluhakemistoa ja hakee oi-
10 kean salasanan palveluhakemiston osoittamasta paikasta. Etsintälohko palauttaa etsimässä salasanana lisäyslohkolle.

Uusien salasanojen lisäyslohko toimii keksinnön parhaassa toteutusmuodossa muista lohkoista täysin
15 riippumattomasti. Käytännössä se tarkkailee SIM-kortille tulevaa TS GSM 11.14 versio 5.1.0 mukaista SMS data Download -liikennettä ja havaitsee uusien salasanojen tupsahtamisen kortille. Uusien salasanojen lisäyslohko tallettaa SMS Data Download -sanomassa
20 tulleet uudet salasanat sopivaan erikoistiedostoon SIM-kortille ja tekee asianmukaisen lisäyksen palveluhakemistoon, jotta salasanojen etsintälohko löytää uudet salasanat. Tämä uusi salasanatiedosto saattaa olla yhdistelmä, joka sisältää edellisen tiedoston viimei-
25 siä käyttämättömiä salasanoja ja juuri saapuneita kokonaan uusia salasanoja.

Keksintöä ei rajata pelkästään edellä esitettyä sovellutusesimerkkiä koskevaksi, vaan monet muunnokset ovat mahdollisia pysyttäessä patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.
30

PATENTTIVAATIMUKSET

1. Menetelmä palvelun käyttämiseksi tietoliikennejärjestelmässä, jossa palvelun käyttäjälle annetaan joukko kertakäyttöisiä salasanoja, joita käyttäen käyttäjä pääsee käyttämään palvelua tele- ja/tai dataverkon välityksellä, ja jossa menetelmässä päätelaitteella luodaan yhteys palvelinlaitteeseen ja lähetetään salasana palveluun kytkeydyttäessä, tunnistetaan salasana ja sallitaan ja/tai estetään palvelun käyttö annetun salasanan perusteella, tunnettu siitä, että

- tallennetaan päätelaitteeseen salasanajoukko,
- valitaan oikea salasana tallennetusta salasanajoukosta ennalta määrättyyn palveluun kytkeydyttäessä, ja
- liitetään salasana automaattisesti päätelaitteesta palvelinlaitteeseen siirrettävään yhteydenottosignaaliin.

2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että kirjataan salasanajoukosta käytetyt salasanat.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, tunnettu siitä, että päivitetään päätelaitteessa olevaa salasanajoukkoa palvelinlaitteelta tele- ja/tai dataverkon välityksellä.

4. Jonkin patenttivaatimuksista 1 - 3 mukainen menetelmä, tunnettu siitä, että tilataan uusi salasanajoukko automaattisesti palvelinlaitteelta edellisen salasanajoukon tultua käytetyksi.

5. Jonkin patenttivaatimuksista 1 - 4 mukainen menetelmä, tunnettu siitä, että tallennetaan päätelaitteeseen useita eri palveluja vastaavia salasanajoukkoja, ja valitaan yhteydenmuodostuksessa kulloistakin käytettävää palvelua vastaava salasanajoukko.

6. Tietoliikennejärjestelmä, jossa palvelun käyttäjälle annetaan joukko kertakäyttöisiä salasanoja, joita käyttäen käyttäjä pääsee käyttämään palvelua tele- ja/tai dataverkon välityksellä, ja johon järjestelmään kuuluu

- käyttäjän päätelaite, jossa on välineet salasanan lähettämiseksi palveluun kytkeydyttäessä, ja
- palvelinlaite, johon päätelaite luo yhteyden ja johon palvelinlaitteeseen kuuluu välineet salasanan tunnistamiseksi ja palvelun käytön sallimiseksi ja/tai estämiseksi annetun salasanan perusteella, tunnettu siitä, että päätelaitteeseen kuuluu välineet salasanajoukon tallentamiseksi ja oikean salasanan valitsemiseksi tallennetusta salasanajoukosta ennalta määrättyyn palveluun kytkeydyttäessä salasanan automaattiseksi liittämiseksi päätelaitteesta palvelinlaitteeseen siirrettävään yhteydenottosignaaliin.

7. Patenttivaatimuksen 6 mukainen järjestelmä, tunnettu siitä, että päätelaitteeseen kuuluu välineet salasanajoukon käytettyjen salasanojen kirjaamiseksi.

8. Patenttivaatimuksen 6 tai 7 mukainen järjestelmä, tunnettu siitä, että palvelinlaitteeseen kuuluu välineet salasanajoukon päivittämiseksi päätelaitteelle tele- ja/tai dataverkon välityksellä, ja että päätelaitteeseen kuuluu välineet salasanajoukon vastaanottamiseksi.

9. Jonkin patenttivaatimuksista 6 - 8 mukainen järjestelmä, tunnettu siitä, että päätelaitteeseen kuuluu välineet uuden salasanajoukon automaattiseksi tilaamiseksi palvelinlaitteelta edellisen salasanajoukon tultua käytetyksi.

10. Jonkin patenttivaatimuksista 6 - 9 mukainen järjestelmä, tunnettu siitä, että päätelaitteeseen kuuluu välineet useita eri palveluja vastaavien salasanajoukkojen tallentamiseksi.

11. Patenttivaatimuksen 10 mukainen järjestelmä, tunnettu siitä, että päätelaitteeseen kuuluu välineet kulloistakin käytettävää palvelua vastaavan salasanajoukon valitsemiseksi.

5 12. Jonkin patenttivaatimuksista 6 - 11 mukainen järjestelmä, tunnettu siitä, että tietoliikennejärjestelmään kuuluu kiinteä verkko ja päätelaite on kiinteän verkon telepätelaite, kuten puhelin.

10 13. Jonkin patenttivaatimuksista 6 - 12 mukainen järjestelmä, tunnettu siitä, että tietoliikennejärjestelmään kuuluu matkaviestinverkko, kuten GSM-verkko, ja päätelaite on matkaviestin, kuten GSM-puhelin.

15 14. Jonkin patenttivaatimuksista 13 mukainen järjestelmä, tunnettu siitä, että päätelaite on GSM-puhelin, ja että välineet mainittujen salasanojen hallintatoimintojen käyttämiseksi on järjestetty tilaajaintiteettimoduliin, kuten SIM-korttiin.

20 15. Patenttivaatimuksen 14 mukainen järjestelmä, tunnettu siitä, että tilaajaintiteettimodulin ja palvelinlaitteen välisessä yhteydenmuodostuksessa salasanojen välitys on järjestetty soitetun tilaajanumeron avulla.

25 16. Patenttivaatimuksen 14 tai 15 mukainen järjestelmä, tunnettu siitä, että tilaajaintiteettimodulin ohjelmavälineet on järjestetty tunnistamaan palvelun sen tunnistetiedon, kuten puhelinnumeron, perusteella, ja lisäämään yhteydenmuodostuksessa palvelun puhelinnumeron loppuun joukon lisänumeroita, jotka muodostavat salasanan.

30 17. Jonkin patenttivaatimuksista 13 - 16 mukainen järjestelmä, tunnettu siitä, että tilaajaintiteettimoduliin on järjestetty palveluhakemisto, joka sisältää tiedot palveluista, palvelujen tunnistetiedoista ja palvelujen yhteydessä käytettävien salasanatiedostojen nimistä.

18. Patenttivaatimuksen 17 mukainen järjestelmä, tunnettu siitä, että palveluhakemistoon on järjestetty kutakin palvelua varten osoitin, joka on järjestetty osoittamaan salasanajoukon ensimmäistä
5 käyttämätöntä salasanaa ja ko. salasanan tultua käytetyksi siirtymään osoittamaan järjestyksessä seuraavaa käyttämätöntä salasanaa.

19. Jonkin patenttivaatimuksista 13 - 18 mukainen järjestelmä, tunnettu siitä, että välineisiin
10 uusien salasanojen tilaamiseksi ja niiden siirtämiseksi palvelinlaitteen ja tilaajaidentiteettimodulin välillä kuuluu GSM-verkon lyhytsanomapalvelu (SMS-PP-palvelu).

25

(57) TIIVISTELMÄ

Keksinnön kohteena on menetelmä ja tietoliikennejärjestelmä, jossa palvelun tarjoaja antaa palvelun käyttäjälle joukon kertakäyttöisiä salasanoja, joita käyttäen käyttäjä pääsee käyttämään palvelua tele- ja/tai dataverkon välityksellä. Järjestelmään kuuluu käyttäjän päätelaite, jossa on välineet salasanan lähettämiseksi palveluun kytkeydyttäessä, ja palvelinlaite, johon päätelaite luo yhteyden ja johon palvelinlaitteeseen kuuluu välineet salasanan tunnistamiseksi ja palvelun käytön sallimiseksi ja/tai estämiseksi annetun salasanan perusteella. Päätelaitteeseen kuuluu välineet salasanajoukon tallentamiseksi ja oikean salasanan valitsemiseksi tallennetusta salasanajoukosta ennalta määrättyyn palveluun kytkeydyttäessä salasanan automaattiseksi liittämiseksi päätelaitteesta palvelinlaitteeseen siirrettävään yhteydenottosignaaliin.